Terms used
certificate session key product serial number type category

Found **1,303** of **19,243 searched out of 198,991.**

Sort results by relevance

Display results expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale

1 Fast detection of communication patterns in distributed executions

Thomas Kunz, Michiel F. H. Seuren

November 1997 **Proceedings of the 1997 conference of the Centre for Advanced Studies on Collaborative research CASCON '97**

Publisher: IBM Press

Full text available: pdf(4.21 MB) Additional Information: full citation, abstract, references, index terms

Understanding distributed applications is a tedious and difficult task. Visualizations based on process-time diagrams are often used to obtain a better understanding of the execution of the application. The visualization tool we use is Poet, an event tracer developed at the University of Waterloo. However, these diagrams are often very complex and do not provide the user with the desired overview of the application. In our experience, such tools display repeated occurrences of non-trivial commun ...

2 Link and channel measurement: A simple mechanism for capturing and replaying wireless channels

Glenn Judd, Peter Steenkiste

August 2005 **Proceeding of the 2005 ACM SIGCOMM workshop on Experimental approaches to wireless network design and analysis E-WIND '05**

Publisher: ACM Press

Full text available: pdf(6.06 MB) Additional Information: full citation, abstract, references, index terms

Physical layer wireless network emulation has the potential to be a powerful experimental tool. An important challenge in physical emulation, and traditional simulation, is to accurately model the wireless channel. In this paper we examine the possibility of using on-card signal strength measurements to capture wireless channel traces. A key advantage of this approach is the simplicity and ubiquity with which these measurements can be obtained since virtually all wireless devices provide the req ...

Keywords: channel capture, emulation, wireless

3 Frontmatter (TOC, Letters, Election results, Software Reliability Resources!, Computing Curricula 2004 and the Software Engineering Volume SE2004, Software Reuse Research, ICSE 2005 Forward)

July 2005 **ACM SIGSOFT Software Engineering Notes**, Volume 30 Issue 4

Publisher: ACM Press

Full text available: pdf(6.19 MB) Additional Information: full citation, index terms

4 Special issue: AI in engineering

D. Sriram, R. Joobbani
April 1985 **ACM SIGART Bulletin**, Issue 92
Publisher: ACM Press
Full text available: pdf(8.79 MB) Additional Information: full citation, abstract

The papers in this special issue were compiled from responses to the announcement in the July 1984 issue of the SIGART newsletter and notices posted over the ARPAnet. The interest being shown in this area is reflected in the sixty papers received from over six countries. About half the papers were received over the computer network.

5 Frontmatter (TOC, Letters, Philosophy of computer science, Interviewers needed, Taking software requirements creation from folklore to analysis, SW components and product lines: from business to systems and technology, Software engineering survey)

September 2005 **ACM SIGSOFT Software Engineering Notes**, Volume 30 Issue 5
Publisher: ACM Press
Full text available: pdf(1.98 MB) Additional Information: full citation, index terms

6 Computing curricula 2001

September 2001 **Journal on Educational Resources in Computing (JERIC)**
Publisher: ACM Press
Full text available: pdf(613.63 KB) html(2.78 KB) Additional Information: full citation, references, citings, index terms

7 Workshop on compositional software architectures: workshop report

May 1998 **ACM SIGSOFT Software Engineering Notes**, Volume 23 Issue 3
Publisher: ACM Press
Full text available: pdf(2.91 MB) Additional Information: full citation, index terms

8 Automatic parsing for content analysis

Frederick J. Damerau
June 1970 **Communications of the ACM**, Volume 13 Issue 6
Publisher: ACM Press
Full text available: pdf(4.07 MB) Additional Information: full citation, abstract, references, citings

Although automatic syntactic and semantic analysis is not yet possible for all of an unrestricted natural language text, some applications, of which content analysis is one, do not have such a stringent coverage requirement. Preliminary studies show that the Harvard Syntactic Analyzer can produce correct and unambiguous identification of the subject and object of certain verbs for approximately half of the relevant occurences. This provides a degree of coverage for content analysis variable ...

Keywords: content analysis, information retrieval, language analysis, natural language processing, parsing, syntactic analysis, text processing

9 Frontmatter (TOC, Miscellaneous material)

ACM SIGSOFT Software Engineering Notes staff
November 2006 **ACM SIGSOFT Software Engineering Notes**, Volume 31 Issue 6
Publisher: ACM Press
Full text available: pdf(1.25 MB) Additional Information: full citation

10 A methodology for analyzing the performance of authentication protocols

Alan Harbitter, Daniel A. Menascé
November 2002 **ACM Transactions on Information and System Security (TISSEC)**, Volume 5 Issue 4
Publisher: ACM Press
Full text available: pdf(1.25 MB) Additional Information: full citation, abstract, references, index terms

Performance, in terms of user response time and the consumption of processing and communications resources, is an important factor to be considered when designing authentication protocols. The mix of public key and secret key encryption algorithms typically included in these protocols makes it difficult to model performance using conventional analytical methods. In this article, we develop a validated modeling methodology to be used for analyzing authentication protocol features, and we use two ...

Keywords: Authentication, Kerberos, mobile computing, performance modeling, proxy servers, public key cryptography

11 COCA: A secure distributed online certification authority

Lidong Zhou, Fred B. Schneider, Robbert Van Renesse
November 2002 **ACM Transactions on Computer Systems (TOCS)**, Volume 20 Issue 4
Publisher: ACM Press
Full text available: pdf(448.28 KB) Additional Information: full citation, abstract, references, citings, index terms

COCA is a fault-tolerant and secure online certification authority that has been built and deployed both in a local area network and in the Internet. Extremely weak assumptions characterize environments in which COCA's protocols execute correctly: no assumption is made about execution speed and message delivery delays; channels are expected to exhibit only intermittent reliability; and with $3t + 1$ COCA servers up to t may be faulty or compromised. COCA is the first system to integr ...

Keywords: Byzantine quorum systems, Certification authority, denial of service, proactive secret-sharing, public key infrastructure, threshold cryptography

12 Security: Privacy protection for signed media files: a separation-of-duty approach to the lightweight DRM (LWDRM) system

Rüdiger Grimm, Patrick Aichroth
September 2004 **Proceedings of the 2004 workshop on Multimedia and security MM&Sec '04**
Publisher: ACM Press
Full text available: pdf(256.47 KB) Additional Information: full citation, abstract, references, index terms

The aim of strong digital rights management (DRM) is to enforce usage rules in end-user devices on behalf of content providers. Strong DRM is not well accepted by customers. Moreover, strong DRM is repeatedly circumvented and broken. Since Napster (and all its

Peer-to-Peer follow-ups), the Internet is flooded with illegal digital content. We introduce the LWDRM technology as an alternative model. LWDRM relies on responsible behavior of customers. However, LWDRM contains a privacy problem, in tha ...

Keywords: LWDRM, light weight digital rights management, privacy, pseudonyms, separation of duty, virtual goods

13 Authentication and signature schemes: On the performance, feasibility, and use of forward-secure signatures

Eric Cronin, Sugih Jamin, Tal Malkin, Patrick McDaniel

October 2003 **Proceedings of the 10th ACM conference on Computer and communications security CCS '03**

Publisher: ACM Press

Full text available: pdf(386.51 KB) Additional Information: full citation, abstract, references, citings, index terms

Forward-secure signatures (FSSs) have recently received much attention from the cryptographic theory community as a potentially realistic way to mitigate many of the difficulties digital signatures face with key exposure. However, no previous works have explored the practical performance of these proposed constructions in real-world applications, nor have they compared FSS to traditional, non-forward-secure, signatures in a non-asymptotic way.We present an empirical evaluation of several FSS sch ...

Keywords: digital signatures, forward-secure signatures

14 The model, language, and implementation of an object-oriented multimedia knowledge base management system

Hiroshi Ishikawa, Fumio Suzuki, Fumihiko Kozakura, Akifumi Makinouchi, Mika Miyagishima, Yoshio Izumida, Masaaki Aoshima, Yasuo Yamane

March 1993 **ACM Transactions on Database Systems (TODS)**, Volume 18 Issue 1

Publisher: ACM Press

Full text available: pdf(3.23 MB) Additional Information: full citation, abstract, references, citings, index terms, review

New applications such as CAD, AI, and hypermedia require direct representation and flexible use of complex objects, behavioral knowledge, and multimedia data. To this end, we have devised a knowledge base management system called Jasmine. An object-oriented approach in a programming language also seems promising for use in Jasmine. Jasmine extends the current object-oriented approach and provides the following features. Our object model is based on functional data models and well-establis ...

15 Special feature: Report on a working session on security in wireless ad hoc networks

Levente Buttyán, Jean-Pierre Hubaux

January 2003 **ACM SIGMOBILE Mobile Computing and Communications Review**, Volume 7 Issue 1

Publisher: ACM Press

Full text available: pdf(2.50 MB) Additional Information: full citation, references, citings

16 Data base directions: the next steps

John L. Berg

November 1976 **ACM SIGMOD Record , ACM SIGMIS Database**, Volume 8 , 8 Issue 4 , 2

Publisher: ACM Press

Full text available: pdf(9.95 MB) Additional Information: full citation, abstract, citings

What information about data base technology does a manager need to make prudent decisions about using this new technology? To provide this information the National Bureau of Standards and the Association for Computing Machinery established a workshop of approximately 80 experts in five major subject areas. The five subject areas were auditing, evolving technology, government regulations, standards, and user experience. Each area prepared a report contained in these proceedings. The proceedings p ...

Keywords: DBMS, auditing, cost/benefit analysis, data base, data base management, government regulation, management objectives, privacy, security, standards, technology assessment, user experience

17 A model of OASIS role-based access control and its support for active security

Jean Bacon, Ken Moody, Walt Yao
November 2002 **ACM Transactions on Information and System Security (TISSEC)**, Volume 5 Issue 4
Publisher: ACM Press

Full text available: pdf(352.06 KB) Additional Information: full citation, abstract, references, citings, index terms

OASIS is a role-based access control architecture for achieving secure interoperation of services in an open, distributed environment. The aim of OASIS is to allow autonomous management domains to specify their own access control policies and to interoperate subject to service level agreements (SLAs). Services define roles and implement formally specified policy to control role activation and service use; users must present the required credentials, in an appropriate context, in order to activat ...

Keywords: Certificates, OASIS, RBAC, distributed systems, policy, role-based access control, service-level agreements

18 Walter Carlson interview: November 26-27, 2005; Los Gatos, California

Thomas Haigh
January 2006 **ACM Oral History interviews**
Publisher: ACM Press

Full text available: pdf(364.63 KB) Additional Information: full citation, abstract

Walter Carlson discusses his entire career in the computing field. Born in Denver in 1916, Carlson studied Chemical Engineering at the University of Colorado, gaining both bachelors and masters degrees in Chemical Engineering. On graduation Carlson went to work for DuPont, where he worked as part of the corporate Engineering Department to improve industrial processes in different plants. In 1954 his involvement in a feasibility study to investigate computer procurement won Carlson a j ...

19 The automated production control documentation system: a case study in cleanroom software engineering

Carmen J. Trammell, Leon H. Binder, Cathrine E. Snyder
January 1992 **ACM Transactions on Software Engineering and Methodology (TOSEM)**, Volume 1 Issue 1
Publisher: ACM Press

Full text available: pdf(900.71 KB) Additional Information: full citation, abstract, references, citings, index terms, review

A prototype software system was developed for the U.S. Naval Underwater Systems Center(NUSC) as a demonstration of the Cleanroom Software Engineering methodology. The Cleanroom method is a team approach to the incremental development of software

under statistical quality control. Cleanroom's formal methods of Box Structure specification and design, functional verification, and statistical testing were used by a four-person team to develop the Automated Production Control Documentation(APCOD ...

Keywords: box structures, cleanroom software engineering, statistical quality control, statistical testing

20 Practice: Cybercrime, identity theft, and fraud: practicing safe internet - network security threats and vulnerabilities

Robert C. Newman

September 2006 **Proceedings of the 3rd annual conference on Information security curriculum development InfoSecCD '06**

Publisher: ACM Press

Full text available: pdf(123.56 KB) Additional Information: full citation, abstract, references, index terms

Computer networks and computer systems are experiencing attacks and threats from many areas. Threats are also extended to include the individual user's computer assets and resources. Information will be presented on the categories of security and privacy threats, integrity threats, vulnerabilities, delay and denial threats, and intellectual property threats that are being directed towards corporate, educational, governmental, and individual assets.

Keywords: cybercrime, identity theft, internet fraud

Terms used **certificate session key digital rights management** Found **19,243** of **198,991**

Sort results by relevance

Display results expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown Relevance scale

1 Short papers poster session 2: A trustworthy end-to-end key management scheme for digital rights management

Junil Kim, Yeonjeong Jeong, Kisong Yoon, Jaecheol Ryou

October 2006 **Proceedings of the 14th annual ACM international conference on Multimedia MULTIMEDIA '06**

Publisher: ACM Press

Full text available: pdf(269.86 KB) Additional Information: full citation, abstract, references, index terms

Current studies on Digital Rights Management (DRM) have focused on security and encryption as a means of solving the issue of illegal copying by purchasers. In this paper, we propose an end-to-end key management scheme that can cover a content protection on the overall value-chains of content distribution. The proposed scheme can protect digital content from attacks since an encrypted content is sent by a first package server and only DRM client can decrypt the encrypted digital content. It make ...

Keywords: DRM, content protection, key management

2 Security: Privacy protection for signed media files: a separation-of-duty approach to the lightweight DRM (LWDRM) system

Rüdiger Grimm, Patrick Aichroth

September 2004 **Proceedings of the 2004 workshop on Multimedia and security MM&Sec '04**

Publisher: ACM Press

Full text available: pdf(256.47 KB) Additional Information: full citation, abstract, references, index terms

The aim of strong digital rights management (DRM) is to enforce usage rules in end-user devices on behalf of content providers. Strong DRM is not well accepted by customers. Moreover, strong DRM is repeatedly circumvented and broken. Since Napster (and all its Peer-to-Peer follow-ups), the Internet is flooded with illegal digital content. We introduce the LWDRM technology as an alternative model. LWDRM relies on responsible behavior of customers. However, LWDRM contains a privacy problem, in tha ...

Keywords: LWDRM, light weight digital rights management, privacy, pseudonyms, separation of duty, virtual goods

3 DRM experience: Digital rights management in a 3G mobile phone and beyond

Thomas S. Messerges, Ezzat A. Dabbish
October 2003 **Proceedings of the 3rd ACM workshop on Digital rights management DRM '03**
Publisher: ACM Press

Full text available: pdf(306.59 KB) Additional Information: full citation, abstract, references, citings, index terms

In this paper we examine how copyright protection of digital items can be securely managed in a 3G mobile phone and other devices. First, the basic concepts, strategies, and requirements for digital rights management are reviewed. Next, a framework for protecting digital content in the embedded environment of a mobile phone is proposed and the elements in this system are defined. The means to enforce security in this system are described and a novel "Family Domain" approach to content management ...

Keywords: MPEG-21, copyright protection, cryptography, digital content, digital rights management, embedded system, key management, mobile phone, open mobile alliance, security

4 Applications and compliance: Virtual monotonic counters and count-limited objects using a TPM without a trusted OS

Luis F. G. Sarmenta, Marten van Dijk, Charles W. O'Donnell, Jonathan Rhodes, Srinivas Devadas
November 2006 **Proceedings of the first ACM workshop on Scalable trusted computing STC '06**
Publisher: ACM Press
Full text available: pdf(447.59 KB) Additional Information: full citation, abstract, references, index terms

A trusted monotonic counter is a valuable primitive that enables a wide variety of highly scalable offline and decentralized applications that would otherwise be prone to replay attacks, including offline payment, e-wallets, virtual trusted storage, and digital rights management (DRM). In this paper, we show how one can implement a very large number of *virtual* monotonic counters on an untrusted machine with a Trusted Platform Module (TPM) or similar device, without relying on a trusted OS ...

Keywords: certified execution, e-wallet memory integrity checking, key delegation, stored-value, trusted storage

5 Architechture: Towards an open, trusted digital rights management platform

Andrew Cooper, Andrew Martin
October 2006 **Proceedings of the ACM workshop on Digital rights management DRM '06**
Publisher: ACM Press
Full text available: pdf(417.51 KB) Additional Information: full citation, abstract, references, index terms

Trusted computing has received criticism from those who fear it will be used by influential market forces to exert power over the software used on consumer platforms. This paper describes an open architecture for digital rights management (DRM) enforcement on trusted computing platforms that empowers the consumer to select their operating-system and applications, including open-source options, without weakening the strength of the security functions. A key component in the architecture is a secu ...

Keywords: DRM, digital rights management, mandatory access controls, trusted computing, virtual machines

6

DRM usability and legal issues: Import/export in digital rights management
Reihaneh Safavi-Naini, Nicholas Paul Sheppard, Takeyuki Uehara
October 2004 **Proceedings of the 4th ACM workshop on Digital rights management DRM '04**
Publisher: ACM Press

Full text available: pdf(211.60 KB) Additional Information: full citation, abstract, references, citings, index terms

The inherently controlled nature of digital rights management systems does little to promote inter-operability of systems provided by different vendors. In this paper, we consider import and export functionality by which multimedia protected by one digital rights management regime can be made available to a multimedia device that supports a different digital rights management regime, without compromising the protection afforded to the content under the original regime. We first identify speci ...

Keywords: digital rights management, export, import, inter-operability

7 Full papers (written in English): Prototyping a novel platform for free-trade of digital content
Renan G. Cattelan, Shan He, Darko Kirovski
November 2006 **Proceedings of the 12th Brazilian symposium on Multimedia and the web WebMedia '06**
Publisher: ACM Press

Full text available: pdf(502.96 KB) Additional Information: full citation, abstract, references, index terms

The widespread use of mobile, personal computing devices, together with recent advances in wireless communication technologies, pose a myriad of new opportunities for leveraging the commerce of digital goods. We envision a novel platform for the free-trade of digital content where users are allowed to market and resell copies of digital content to others in their wireless vicinity. By keeping significant part of the revenues, users are likely to drive the sales for their and copyright holders' e ...

Keywords: digital content trading, electronic commerce, mobile commerce, mobile electronic marketing, off-line economies, viral marketing, word-of-mouth

8 Terra: a virtual machine-based platform for trusted computing
Tal Garfinkel, Ben Pfaff, Jim Chow, Mendel Rosenblum, Dan Boneh
October 2003 **ACM SIGOPS Operating Systems Review , Proceedings of the nineteenth ACM symposium on Operating systems principles SOSP '03**, Volume 37 Issue 5
Publisher: ACM Press

Full text available: pdf(140.31 KB) Additional Information: full citation, abstract, references, citings, index terms

We present a flexible architecture for trusted computing, called Terra, that allows applications with a wide range of security requirements to run simultaneously on commodity hardware. Applications on Terra enjoy the semantics of running on a separate, dedicated, tamper-resistant hardware platform, while retaining the ability to run side-by-side with normal applications on a general-purpose computing platform. Terra achieves this synthesis by use of a *trusted virtual machine monitor* (TVMM ...

Keywords: VMM, attestation, authentication, trusted computing, virtual machine, virtual machine monitor

9

Architechture: Towards a secure and interoperable DRM architecture
Gelareh Taban, Alvaro A. Cárdenas, Virgil D. Gligor
October 2006 **Proceedings of the ACM workshop on Digital rights management DRM '06**
Publisher: ACM Press
Full text available: pdf(442.79 KB) Additional Information: full citation, abstract, references, index terms

In this paper we look at the problem of interoperability of digital rights management (DRM)systems in home networks. We introduce an intermediate module called the Domain Interoperability Manager (DIM) to efficiently deal with the problem of content and license translation across different DRM regimes. We also consider the threat model specific to interoperability systems, and introduce threats such as the cross-compliancy and splicing attacks. We formalize the adversary model and define securit ...

Keywords: DRM, home networks, interoperability

10 Security in embedded systems: Design challenges
Srivaths Ravi, Anand Raghunathan, Paul Kocher, Sunil Hattangady
August 2004 **ACM Transactions on Embedded Computing Systems (TECS)**, Volume 3 Issue 3
Publisher: ACM Press
Full text available: pdf(3.67 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Many modern electronic systems---including personal computers, PDAs, cell phones, network routers, smart cards, and networked sensors to name a few---need to access, store, manipulate, or communicate sensitive information, making security a serious concern in their design. Embedded systems, which account for a wide range of products from the electronics, semiconductor, telecommunications, and networking industries, face some of the most demanding security concerns---on the one hand, they are oft ...

Keywords: Embedded systems, architecture, authentication, battery life, cryptographic algorithms, decryption, encryption, hardware design, processing requirements, security, security attacks, security protocols, tamper resistance

11 Information protection methods: Display-only file server: a solution against information theft due to insider attack
Yang Yu, Tzi-cker Chiueh
October 2004 **Proceedings of the 4th ACM workshop on Digital rights management DRM '04**
Publisher: ACM Press
Full text available: pdf(311.80 KB) Additional Information: full citation, abstract, references, index terms

Insider attack is one of the most serious cybersecurity threats to corporate America. Among all insider threats, information theft is considered the most damaging in terms of potential financial loss. Moreover, it is also especially difficult to detect and prevent, because in many cases the attacker has the proper authority to access the stolen information. According to the 2003 CSI/FBI Computer Crime and Security Survey, theft of proprietary information was the single largest category of los ...

Keywords: access, digital rights management, information theft, insider attack

12 Trustworthy systems: Property-based attestation for computing platforms: caring about properties, not mechanisms

Ahmad-Reza Sadeghi, Christian Stüble
September 2004 **Proceedings of the 2004 workshop on New security paradigms NSPW '04**
Publisher: ACM Press
Full text available: pdf(222.19 KB) Additional Information: full citation, abstract, references, citings

Over the past years, the computing industry has started various initiatives announced to increase computer security by means of new hardware architectures. The most notable effort is the Trusted Computing Group (TCG) and the Next-Generation Secure Computing Base (NGSCB). This technology offers useful new functionalities as the possibility to verify the integrity of a platform (attestation) or binding quantities on a specific platform (sealing).In this paper, we point out the deficiencies of the ...

13 Systems and architectures: A DRM security architecture for home networks

Bogdan C. Popescu, Bruno Crispo, Andrew S. Tanenbaum, Frank L.A.J. Kamperman
October 2004 **Proceedings of the 4th ACM workshop on Digital rights management DRM '04**
Publisher: ACM Press
Full text available: pdf(222.46 KB) Additional Information: full citation, abstract, references, citings, index terms

This paper describes a security architecture allowing digital rights management in home networks consisting of consumer electronic devices. The idea is to allow devices to establish dynamic groups, so called "Authorized Domains", where legally acquired copyrighted content can seamlessly move from device to device. This greatly improves the end-user experience, preserves "fair use" expectations, and enables the development of new business models by content providers. Key to our design is a hyb ...

Keywords: DRM architectures, compliant CE devices, digital content protection

14 Digital multimedia book: From digital audiobook to secure digital multimedia-book

Lavinia Egidi, Marco Furini
July 2006 **Computers in Entertainment (CIE)**, Volume 4 Issue 3
Publisher: ACM Press
Full text available: pdf(364.18 KB) Additional Information: full citation, abstract, references, index terms

Portable devices and wireless connections are creating a new scenario in which digital information is entering our lives in a massive way. In this article we consider MP3 audiobook applications and propose an approach to completely restyle the applications to the current mobile and multimedia scenario. Our mechanism introduces multimedia contents (images and text) into the audiobook application and synchronizes them with the MP3 audio stream. Multimedia contents are protected by a security syste ...

Keywords: multimedia applications, multimedia communications, multimedia over wireless, music distribution

15 Session 3: XML applications: XrML -- eXtensible rights Markup Language

Xin Wang, Guillermo Lao, Thomas DeMartini, Hari Reddy, Mai Nguyen, Edgar Valenzuela
November 2002 **Proceedings of the 2002 ACM workshop on XML security XMLSEC '02**
Publisher: ACM Press
Full text available: pdf(466.82 KB) Additional Information: full citation, abstract, references, citings, index terms, review

XrML (eXtensible rights Markup Language) is an XML-based language for digital rights management (DRM), providing a universal method for specifying rights and conditions

associated with the use and protection of digital content and services. Originally developed at Xerox's Palo Alto Research Center (PARC), the specification facilitates the creation of an open architecture for digital rights management of content or services. It can be integrated with both existing and new DRM systems. XrML is a g ...

Keywords: DRM, XML, content distribution and usage, digital rights management, rights, specification languages, standards

16 Security as a new dimension in embedded system design: Security as a new dimension in embedded system design

Srivaths Ravi, Paul Kocher, Ruby Lee, Gary McGraw, Anand Raghunathan
June 2004 **Proceedings of the 41st annual conference on Design automation DAC '04**
Publisher: ACM Press

Full text available: pdf(209.10 KB) Additional Information: full citation, abstract, references, citings, index terms

The growing number of instances of breaches in information security in the last few years has created a compelling case for efforts towards secure electronic systems. Embedded systems, which will be ubiquitously used to capture, store, manipulate, and access data of a sensitive nature, pose several unique and interesting security challenges. Security has been the subject of intensive research in the areas of cryptography, computing, and networking. However, despite these efforts, *security is ...*

Keywords: *PDAs, architectures, battery life, cryptography, design, design methodologies, digital rights management, embedded systems, performance, security, security processing, security protocols, sensors, software attacks, tamper resistance, trusted computing, viruses*

17 The $UCON_{ABC}$ usage control model

Jaehong Park, Ravi Sandhu
February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 1
Publisher: ACM Press

Full text available: pdf(518.61 KB) Additional Information: full citation, abstract, references, citings, index terms

In this paper, we introduce the family of $UCON_{ABC}$ models for usage control (UCON), which integrate *Authorizations (A), oBligations (B), and Conditions (C)*. We call these core models because they address the essence of UCON, leaving administration, delegation, and other important but second-order issues for later work. The term usage control is a generalization of access control to cover authorizations, obligations, conditions, continuity (ongoing controls), and mutability. Trad ...

Keywords: access control, digital rights management, privacy, trust, usage control

18 Synopsis - Books and Software: iTV handbook: technologies & standards

Eddie Schwalb
April 2004 **Computers in Entertainment (CIE)**, Volume 2 Issue 2
Publisher: ACM Press

Full text available: pdf(335.60 KB) Additional Information: full citation, abstract, index terms

Interactive television (iTV) is an evolutionary merging of digital TV and the internet. iTV technology offers new powerful ways for consumers to interact with content and service

providers. In Europe, iTV has gained significant traction during the turn of the century. For example, about 500,000 viewers signed up for SkyDigital's email service during 2000. In another example, Nickelodeon's "Watch Your Own Week" voting application was available to SkyDigital viewers during Oct 22-27 2001. While on ...

Keywords: QuickTime, avi, broadcast, compression, digital tv, gif, interactive tv, internet, media streaming, mp3, network file system, zip

19 Cryptographic tools: ID-based encryption for complex hierarchies with applications to forward security and broadcast encryption

Danfeng Yao, Nelly Fazio, Yevgeniy Dodis, Anna Lysyanskaya

October 2004 **Proceedings of the 11th ACM conference on Computer and communications security CCS '04**

Publisher: ACM Press

Full text available: pdf(220.00 KB) Additional Information: full citation, abstract, references, index terms

A forward-secure encryption scheme protects secret keys from exposure by evolving the keys with time. Forward security has several unique requirements in hierarchical identity-based encryption (HIBE) scheme: (1) users join dynamically; (2) encryption is joining-time-oblivious; (3) users evolve secret keys autonomously.

We present a scalable forward-secure HIBE (fs-HIBE) scheme satisfying the above properties. We also show how our fs-HIBE scheme can be used to construct a forward-secure ...

Keywords: ID-Based encryption, broadcast encryption, forward security

20 DRM, trusted computing and operating system architecture

Jason F. Reid, William J. Caelli

January 2005 **Proceedings of the 2005 Australasian workshop on Grid computing and e-research - Volume 44 ACSW Frontiers '05**

Publisher: Australian Computer Society, Inc.

Full text available: pdf(191.31 KB) Additional Information: full citation, abstract, references, index terms

Robust technological enforcement of DRM licenses assumes that the prevention of direct access to the raw bit representation of decrypted digital content and the license enforcement mechanisms themselves is possible. This is difficult to achieve on an open computing platform such as a PC. Recent trusted computing initiatives namely, the Trusted Computing Group (TCG) specification, and Microsoft's Next Generation Secure Computing Base (NGSCB) aim in part to address this problem. The protection arc ...

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Web

Results 1 - 10 of about 769 for certificate, "session key", "drm". (0.24 seconds)

[DOC] Robustness Rules for Microsoft Device Bridge For Windows Media DRM
File Format: Microsoft Word - View as HTML
"Device Certificate" means a digital certificate assigned to a Licensed Product and ...
"MSDB Content Key" means the Content Key and the MSDB Session Key. ...
wmlicense.smdisp.net/wmdrmcompliance/doc/Robustness%20Rules%20for%20Microsoft%20Device%20Bridge%20for%20W... - Similar pages

Online CA - Get Free digital certificate. Free Email Certificate ...
Document rights management, DRM. Issues Free certificates ... the customer's Web browser generates a unique "session key" to encrypt all communications with ...
www.ascertia.com/OnlineCA/ssl.aspx?linkID=40 - 34k - Cached - Similar pages

> Online CA - Get Free digital certificate. Free Email Certificate ...
> Document rights management, DRM. Issues Free certificates ... She then encrypts this session key with Bob's public key (so only he can read it) and encrypts ...
> www.ascertia.com/OnlineCA/cryptography.aspx?linkID=40 - 35k - Cached - Similar pages

[PDF] A proposal on open DRM system coping with both benefits of rights ...
File Format: PDF/Adobe Acrobat
inputs License Certificate File to the Open DRM System. instead of License File. ...
enciphers a Protect Key with the session key to be sent to ...
ieeexplore.ieee.org/iel5/8900/28138/01259001.pdf - Similar pages

[Paper] License Administration Mechanism for Multiple Devices in a ...
The goals of this registration procedure are to register the DRM client identifier, the DRM client's certificate and the DRM client's device capability ...
www.actapress.com/PDFViewer.aspx?paperId=16633 - Similar pages

Creating and Initializing a DRM Writer
Encrypt the session key with the public key extracted from the certificate. Fill out a WMDRM_IMPORT_INIT_STRUCT structure. ...
msdn2.microsoft.com/en-us/library/aa384802.aspx - 11k - Cached - Similar pages

[PDF] Fraunhofer Institute for Digital Media Technology IDMT
File Format: PDF/Adobe Acrobat - View as HTML
2. AES decryption with. symmetric session key. User Certificate. P2P Signaling ... It is not up to DRM technology to decide what. is legal, and what is not. ...
web.cs.missouri.edu/~zeng/CCNC05DRM/CCNC05_LWDRM_Aichroth.pdf - Similar pages

Microsoft's Digital Rights Management Scheme - Technical Details
Several key DLLs are kept in \windows\system that relate to the MS-DRM scheme. ... which make up an ECC encrypted random session key, and the remaining 88 ...
cryptome.org/ms-drm.htm - 46k - Cached - Similar pages

Digital rights management - US Patent 7036011
encrypting the random session key with the public key of the PKI key pair. ... the DRM determines if the digital certificate is valid by retrieving the copy ...
www.patentstorm.us/patents/7036011-claims.html - 22k - Cached - Similar pages

Windows Media DRM FAQ

After being authorized, the company is provided with a **certificate**, which can be revoked if their player is compromised. Windows Media **DRM** run-time software ...
www.microsoft.com/windows/windowsmedia/forpros/**drm**/faq.aspx - 59k -
Cached - Similar pages

Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**

---

certificate, "session key", "drm" Search

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

---

Google Home - Advertising Programs - Business Solutions - About Google

Web Results **1 - 10** of about **617** for **certificate, "media player", "session key"**. (**0.11** seconds)

Windows Media DRM FAQ
The authentication protocol also establishes a **session key**, ... Windows **Media Player** 6.4 can use this URL to acquire a version 1 license for the content or ...
www.microsoft.com/windows/windowsmedia/forpros/drm/faq.aspx - 59k - Cached - Similar pages

Microsoft's Digital Rights Management Scheme - Technical Details
Simply use the MS **Media player**, have it request and decrypt the licenses, ... which make up an ECC encrypted random **session key**, and the remaining 88 bytes ...
cryptome.org/ms-drm.htm - 46k - Cached - Similar pages

Glossary
Private keys are typically used to encrypt a symmetric **session key**, ... such as a network login, hardware ID, or **certificate**, to a message, file, ...
msdn2.microsoft.com/en-us/library/bb263170.aspx - 26k - Cached - Similar pages

[DOC] Legal Notice
File Format: Microsoft Word - View as HTML
The licensing agreement explains how to get a device **certificate**. ... To learn more about Windows **Media Player**, see Windows **Media Player** Help. ...
download.microsoft.com/download/3/a/f/3afb9301-5ade-4247-98ba-7a06efb75168/Introducing_Janus_and_Cardea.doc - Similar pages

> [DOC] Legal Notice
> File Format: Microsoft Word - View as HTML
> A component of the **media player** requests the public key from the device, ... encrypted **session key**, a rights policy statement specifying the security ...
> download.microsoft.com/.../A_Technical_Overview_of_WM_DRM_10_for_Devices.doc - Similar pages
> [More results from download.microsoft.com]

HotOS IX — Paper
If the CPU evicts a block of the plaintext to external memory, the kernel's trap handler uses a **session key** that the **media player** generated to encrypt the ...
www.usenix.org/events/hotos03/tech/full_papers/chenb/chenb_html/index.html - 38k - Cached - Similar pages

[PDF] Certifying Program Execution with Secure Processors
File Format: PDF/Adobe Acrobat - View as HTML
loader, µ-kernel, and **media player**). A distributor can. discover a Cerium computer's configuration from a. **certificate** signed by the computer's secure CPU. ...
pdos.csail.mit.edu/papers/cerium:hotos03.pdf - Similar pages

[Paper] License Administration Mechanism for Multiple Devices in a ...
The **certificate** would be signed by a CA. The **certificate** chain is ... On receipt of the second message, C acquires the **session key** K . He then checks the ...
www.actapress.com/PDFViewer.aspx?paperId=16633 - Similar pages

[PDF] Multimedia rights management for the multiple devices of end-user ...
File Format: PDF/Adobe Acrobat

management and the **certificate** distribution as trusted ... keys and the contents service **session key** are assumed to. be bits in length. ...
ieeexplore.ieee.org/iel5/8560/27094/01203625.pdf - Similar pages

[PDF] Off-line Economies for Digital Media
File Format: PDF/Adobe Acrobat - View as HTML
on-line store, iTunes, with a **media player** device, the iPod ... encrypted with a **session key** derived from the session mas-. ter key (created in step I). ...
research.microsoft.com/users/darkok/papers/nossdav.pdf - Similar pages

Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**

Results for "((certificate<in>metadata) <and> (session key<in>metadata))" e-mail
Your search matched 7 of 1527266 documents.
A maximum of 100 results are displayed, 25 to a page, sorted by Relevance in Descending order.

» Search Options

View Session History

New Search

Modify Search

((certificate<in>metadata) <and> (session key<in>metadata)) Search

Check to search only within this results set

Display Format: Citation Citation & Abstract

» Key

IEEE JNL	IEEE Journal or Magazine
IET JNL	IET Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IET CNF	IET Conference Proceeding
IEEE STD	IEEE Standard

view selected items Select All Deselect All

1. **On certificate-based security protocols for wireless mobile communicatic**
Chang-Seop Park;
Network, IEEE
Volume 11, Issue 5, Sept.-Oct. 1997 Page(s):50 - 55
Digital Object Identifier 10.1109/65.620522
AbstractPlus | Full Text: PDF(1492 KB) IEEE JNL
Rights and Permissions

2. **Design of key recovery system using multiple agent technology for electi**
Shin-Young Lim; Ho-Sang Hani; Myoung-Jun Kim; Tai-Yun Kim;
Industrial Electronics, 2001. Proceedings. ISIE 2001. IEEE International Sympo
Volume 2, 12-16 June 2001 Page(s):1351 - 1356 vol.2
Digital Object Identifier 10.1109/ISIE.2001.931678
AbstractPlus | Full Text: PDF(464 KB) IEEE CNF
Rights and Permissions

3. **Key-exchange authentication using shared secrets**
Badra, M.; Hajjeh, I.;
Computer
Volume 39, Issue 3, March 2006 Page(s):58 - 66
Digital Object Identifier 10.1109/MC.2006.94
AbstractPlus | Full Text: PDF(680 KB) IEEE JNL
Rights and Permissions

4. **Mutual Authentication and Key Agreement for GSM**
K.Phani Kumar; G. Shailaja; A. Kavitha; Ashutosh Saxena;
Mobile Business, 2006. ICMB '06. International Conference on
June 2006 Page(s):25 - 25
Digital Object Identifier 10.1109/ICMB.2006.37
AbstractPlus | Full Text: PDF(198 KB) IEEE CNF
Rights and Permissions

5. **TAKCS: threshold authentication key configuration scheme for multilaye mobile ad hoc networks**
Keun-Ho Lee; Chong-Sun Hwang;
Advanced Communication Technology, 2006. ICACT 2006. The 8th Internatior
Volume 1, 20-22 Feb. 2006 Page(s):6 pp.

AbstractPlus | Full Text: PDF(5000 KB) IEEE CNF
Rights and Permissions

6. **Password-authenticated 3PEKE with round efficiency without server's pu**
Ya-Fen Chang; Chin-Chen Chang;
Cyberworlds, 2005. International Conference on
23-25 Nov. 2005 Page(s):5 pp.
Digital Object Identifier 10.1109/CW.2005.70
AbstractPlus | Full Text: PDF(184 KB) IEEE CNF
Rights and Permissions

7. **Protecting all traffic channels in mobile IPv6 network**
Ying Qiu; Jianying Zhou; Feng Bao;
Wireless Communications and Networking Conference, 2004. WCNC. 2004 IE
Volume 1, 21-25 March 2004 Page(s):160 - 165 Vol.1
AbstractPlus | Full Text: PDF(338 KB) IEEE CNF
Rights and Permissions